AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATIONS

I, Derek Dunn, being duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of applications for the following:

a. A search warrant for information associated with WhatsApp account numbers (978)677-0918 and (508)581-7272 that is stored at premises controlled by WhatsApp Inc. of Menlo Park, California. The information to be searched is described in the following paragraphs and Attachment A1;

b. A search warrant for information associated with TextNow account number (518)730-9917 that is stored at premises controlled by TextNow Inc. of Waterloo, Ontario, Canada[1]. The information to be searched is described in the following paragraphs and Attachment A2;

c. A search warrant for information associated with email address shawnwalker909@yahoo.com that is stored at premises controlled by Oath Holdings Inc. of Sunnyvale, California. The information to be searched is described in the following paragraphs and Attachment A3;

[1] On 07/12/2019, HSI IRS Lisa LaForte received a response to an administrative Subpoena from TextNow Inc. which included four spreadsheets of information labelled as "subscriber", "ips", "messages", and "calls". Upon IRS Laforte's review of the information in each spreadsheet, she noticed that the spreadsheet labelled "Messages" included what appeared to be text message content associated with the target phone number. IRS LaForte stopped reviewing the information in the "messages" spreadsheet and notified SA Derek Dunn who advised that he would contact AUSA Charles Rombeau and inquire whether the message content could be reviewed since it was voluntarily provided TextNow Inc. or if a Search Warrant would be needed to review this information. AUSA Rombeau subsequently advised SA Dunn to not review the message content and that he would like to obtain the information from TextNow Inc. via Search Warrant.

d. A search warrant for information associated with email address kotara56@gmail.com that is stored at premises controlled by Google LLC of Mountain View, California. The information to be searched is described in the following paragraphs and Attachment A4;

e. A search warrant for information associated with email address kotara1956@sbcglobal.net and account number (210) 827-8958 that is stored at premises controlled by AT&T of North Palm Beach, Florida. The information to be searched is described in the following paragraphs and Attachment A5; and,

f. A search warrant for information associated with email addresses info.GCFCS@usa.com, RC.Officer.R.Breat@deliveryman.com, U.S.ARMY-leavedept@usa.com, and U.S.Custom-Dept@usa.com that is stored at premises controlled by 1&1 Mail & Media Inc of Chesterbrook, Pennsylvania. The information to be searched is described in the following paragraphs and Attachment A6.

2. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and have been so employed since April 2003. I am currently assigned to the Manchester, New Hampshire field office. As part of my regular duties as an agent, I investigate criminal violations relating to a broad range of immigration and customs related statutes, including those relating to financial crimes. During my career, I have conducted and assisted in several investigations of financial related crimes and have received specific training regarding these crimes during my tenure as a Special Agent.

3. I am a "Federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. The information contained in this affidavit is based on information conveyed to me by other law enforcement officials, and my review of records, documents and other physical evidence obtained during this investigation.

5. This affidavit contains information necessary to support probable cause for this application. This affidavit is not intended to include each and every fact or matter observed by me or known to the government. Based on my training and experience and the facts as set forth in this affidavit, I submit that the facts set forth in this affidavit establish probable cause to believe that violations of 18 U.S.C. § 134 (wire fraud) been committed and that WhatsApp account numbers (978)677-0918 and (508)581-7272, TextNow account number (518)730-9917, and email addresses shawnwalker909@yahoo.com, info.GCFCS@usa.com, RC.Officer.R.Breat@deliveryman.com, U.S.ARMY-leavedept@usa.com, and U.S.Custom-Dept@usa.com were used by the individual(s) who committed and/or conspired to commit these offenses. I further submit that the individual(s) who committed and/or conspired to commit these offenses utilized these accounts to communicate with a victim of these crimes who utilized email addresses kotara56@gmail.com and kotara1956@sbcglobal.net and phone number (210)827-8958. Accordingly, I submit that there is probable cause to believe that records and other information associated with all of the accounts identified above contain evidence and fruits of violations of 18 U.S.C. § 1343, as set forth below.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a "district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(ii).

7. The investigation involves offenses within the jurisdiction and proper venue of the United States District Court for the District of New Hampshire, because the accounts at issue are available via the Internet and/or cellular service and therefore accessible within the District of New Hampshire and elsewhere. See 18 U.S.C. § 3237(a); see also 18 U.S.C. §§ 3231 and 3232. Accordingly, the District of New Hampshire has proper venue over the case.

RELEVANT STATUTES

8. This investigation concerns alleged violations of Title 18, United States Code, Sections 1343, related to wire fraud which prohibits a person from devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

PROBABLE CAUSE

BORDER SEARCH OF SUNNA SEPETU

9. On December 23, 2018, Sunna SEPETU, along with two other individuals arrived in a vehicle at the Highgate Springs, Vermont, U.S. Port of Entry to make entry into the U.S. from Canada. During routine questioning, a U.S. Customs and Border Protection (USCBP) Officer detected a strong odor of marijuana coming from the vehicle which resulted in all three

individuals being referred to secondary inspection. During the inspection of the vehicle, a copy of a Bank of America wire transfer dated December 21, 2018 for $30,000 dollars was found. The wire transfer was requested by SEPETU and sent from a bank account in the name of Logitech Group LLC to a bank account in England in the name of Sigma PlantFinder Ltd. There was also a receipt for a financial transfer dated December 21, 2018 for $13,000 dollars from one Bank of America account to another.

10. A basic search was then conducted on two cell phones belonging to SEPETU identified as an iPhone X with telephone number telephone number (978) 677-0918 (i.e., Attachment A1) and a Samsung SM-G930V with telephone number (339) 224-0397. The search of SEPETU's iPhone X revealed numerous photos of bank records showing large currency transfers between Logitech Group LLC and various banks throughout the world totaling more than $300,000 in transactions since October 2018. In addition, USCBP Officers found communications between SEPETU and an individual associated with phone number (508) 581-7272 (i.e., Attachment A1) who was subsequently identified as Nafis QUAYE. Within these communications, which were done through WhatsApp, QUAYE provided SEPETU information on where to wire transfer money to include account names, account numbers, and amounts to wire transfer. On multiple occasions, SEPETU replied to QUAYE with photos of the wire transfer record after it had been made by SEPETU. At one point during these communications, SEPETU asked QUAYE "What's the estimated gross income a year of the business. I have no idea when they ask."

11. When questioned about the financial transactions, SEPETU informed USCBP Officers that she is the owner of Logitech Group LLC and that she has ten employees. SEPETU stated that she has had the business for two years but has not filed taxes. SEPETU stated that she

runs the business out of her house and that she sells computers, printers, and electronics to customers in Nigeria, Tanzania, and Ghana. SEPETU stated that she ships the computers and accessories out via shipping container.

12. Pursuant to open source checks, USCBP Officers found that according to New Hampshire Secretary of State records, Logitech Group LLC was established on 08/16/2017; however, the company was not currently in good standing with the New Hampshire Secretary of State. Further, Sigma PlantFinder Ltd identifies itself as a seller of used large construction machinery to customers worldwide and does not appear to have any association with the sale of computers, printers, and/or electronics.

13. Based on the above, USCBP Officers contacted HSI Special Agent Michael Mccullagh of the Burlington, Vermont office who detained the phones for the purposes of conducting a more thorough border search. SA McCullagh obtained a data extraction from both of SEPETU's cell phones. SEPETU's cell phones along with a hard drive containing the data extractions were then forwarded to me. I subsequently made contact with SEPETU who agreed to come into the HSI Manchester, NH office to pick up her two cell phones.

INTERVIEWS OF SUNNA SEPETU

14. On February 4, 2019, SEPETU came to the HSI Manchester, NH office and met with Special Agent Ronald Morin and I. SEPETU was advised that a border search of her cell phones that had been detained pursuant to her border crossing into the U.S. from Canada on December 23, 2018 had revealed some information that HSI has concerns with, specifically, information relating to her company Logitech Group LLC. SEPETU was asked if she could provide information relating to Logitech Group LLC. SEPETU stated that she is the owner of the company and that she sells computer parts to customers overseas. She advised that she

operates out of her residence and does not actually take possession of any of the items she sells but instead buys computer parts from vendors in other countries (Italy and China) and has the items shipped directly to customers in Africa.

15. SEPETU was asked why she would have made multiple large dollar wire transfers within the past several months from her company bank account to companies that do not appear to sell computer parts such as Sigma PlantFinder and Kleyn Trucks. SEPETU responded that she sells other equipment and pretty much anything at the request of her customers in Africa. She confirmed that the wire transfers to Sigma PlantFinder were for a "Crusher" which is a large machine that digs up roadways and that it was shipped to a customer of hers in Ghana. SEPETU was asked who the customer in Ghana was that purchased the machine, how much profit Logitech Group LLC was making from the sale, and how the customer in Ghana paid Logitech Group LLC for the purchase. SEPETU stated that the customer would have wired funds into her bank account but she could not provide any details relating to the customer name or an estimate on how much profit she made on the sale other than "not very much". She further stated that she typically makes minimal profits and provided an example that she might make $2,000 in profit on a $8,000 sale.

16. When asked further details regarding her business activity to include her customers and how they pay her company, she could only provide minimal details and stated that her friend, subsequently identified as QUAYE, has more knowledge about the business and is the person who sets up the sales and knows the purchasers. SEPETU could not provide an estimate for her sales volume or profits in 2018 or years prior and did not file 2017 taxes for the company. She stated that the only bank account she has for the company is with Bank of America and that she used to have an account with Santander but the account is no longer used.

17. SEPETU was advised that her lack of knowledge of the own company's business in conjunction with her lack of knowledge of her customers is concerning. SEPETU stated that she is learning as she goes with her business and denied that her business was being used for any illicit activity.

18. SEPETU was asked if she could provide copies of her bank statements for the past 6 months as well as copies of all invoices during this time frame for purchases and sales made by her company. SEPETU agreed and stated that she would meet with HSI again after she obtains the documentation requested. Prior to departing, SEPETU's iPhone X and Samsung SM-G930V were returned to her.

19. On February 15, 2019, SEPETU came to the HSI Manchester, NH Office and met with Intelligence Research Specialist (IRS) Lisa Laforte and I. SEPETU provided copies of her monthly statements for Bank of America account number 388004018626 in the name of Logitech Group LLC for the period covering October 1, 2018 through January 31, 2019. Intelligence Research Specialist Laforte conducted a quick review of the bank statements and did not identify any wire transfers from customers in Africa as credits to the account. The majority of the credits to the account appeared to be wire transfers from a USAA Federal Savings Bank account in the name of a female hereinafter referred to as VICTIM1. When asked about VICTIM1, SEPETU had very little information about who she was or where she was located.

20. In addition to the bank statements, SEPETU provided copies of three invoices for items purchased by her company which are summarized as follows:

- Invoice dated 01/05/2019 from La Vita Express of Modena, Italy issued to Shop Car Parts Ghana Ltd of Mataheko, Ghana in the amount of 95,800 EURO for Used Car Engines and Used Suspensions.

- Invoice dated 01/05/2019 from La Vita Express of Modena, Italy issued to Shop Car Parts Ghana Ltd of Mataheko, Ghana in the amount of 34,600 EURO for Various Body and Interior Parts.
- Invoice dated 12/20/2018 from Sigma Plantfinder issued to First Core Quarry Limited of Accra, Ghana in the amount of 232,300 EURO for Used Terex Finlay I100RS tracked impact crusher.

21. SEPETU was asked about invoices or documentation between Logitech Group LLC and its customers in Ghana referencing the transactions as well as other invoices that she did not provide for items purchased by her company. For example, she did not provide an invoice from Kleyn Trucks although her bank records showed a wire transfer made to Kleyn Trucks on 10/03/2018 in the amount of $25,000. SEPETU stated that she did not have any other paperwork but that she would contact QUAYE to see what he has since he is primarily involved with the customers in Ghana.

22. SEPETU subsequently contacted me and advised that she did not have any other paperwork that she could provide. SEPETU was asked how she could not have any paperwork that reflects how much profit her company makes and asked her she will be able to file her taxes without such paperwork. SEPETU stated that she was not sure and would have to figure it out when the time comes.

INTERVIEW WITH VICTIM1

23. On June 13, 2019, Intelligence Research Specialist Laforte, New Hampshire State Police Trooper Tamara Hester, and I telephonically contacted VICTIM1 and inquired about the reason for wire transfers she has made to Logitech Group LLC.

24. VICTIM1 acknowledged that she has sent numerous wire transfers from her bank account to Logitech Group LLC. She advised that the reason she sent the wire transfers was to help a "friend" whom she knows as "Shawn Walker." VICTIM1 met Walker on a dating website approximately 5 years ago after her husband died and she has been in communication with Walker since. VICTIM1's communication with Walker has been primarily via email and text message. VICTIM1 has spoken to Walker on a few occasions over the phone. She stated that he has an accent that sounds German. VICTIM1's understanding is that Walker is currently staying at the Holiday Inn near the airport in Paris, France. VICTIM1 provided the following information about Walker that Walker has provided to her:

Name: Shawn Walker
DOB: [redacted]
Address: [redacted]
Email address: shawnwalker909@yahoo.com (i.e., Attachment A3)
Phone Number: (518)730-9917 (i.e., Attachment A2)

25. VICTIM1 stated that Walker has used the above email address and phone number throughout their communication. VICTIM1 utilized two of her email addresses which she identified as kotara56@gmail.com (i.e., Attachment A4) and kotara1956@sbcglobal.net (i.e., Attachment A5) and has spoken to and text messaged with Walker from her cell phone number of (210)827-8958 (i.e., Attachment A5).

26. VICTIM1 stated that the wire transfers she sent to Logitech Group LLC were at the direction of Walker. VICTIM1's understanding is that Walker has some legal issues relating to some gold bars that he has acquired. VICTIM1 has been wire transferring money to Walker to assist with his legal expenses and estimated that she has sent Walker more than $3 million over the past 5 years. In addition to Logitech Group LLC, VICTIM1 has wire transferred money at

the direction of Walker to other companies as well to include La Vita Express to which she stated that she most recently wire transferred $3,000 just a few days prior.

27. VICTIM1 stated that all of the money she has sent to Walker has been her own money. VICTIM1 has never received money from anyone else for the purpose of sending to Walker.

28. Subsequent to the conversation, VICTIM1 emailed me several photos that she has received from Walker of himself. The photos appeared to be all of the same white male who wears eyeglasses. One of the photos appeared to have the male's face photoshopped onto a male wearing a white t-shirt and holding a white piece of paper with the words "I I LOVE YOU MARYAN". Intelligence Research Specialist Laforte conducted reverse image searches of the Walker photos provided by VICTIM1 and found that some of these photos were reported as being associated with dating app scams involving names other than Walker. Also, Intelligence research Specialist Laforte determined that the photo of Walker holding up a paper with the words "I I LOVE YOU MARYAN" had in fact been photoshopped.

29. Therefore, VICTIM1 appears to have been victimized through a romance scam scheme which induced her to transfer sums of money to Logitech Group LLC under false or fraudulent pretenses.

INTERVIEW WITH VICTIM2

30. On May 13, 2019 and May 19, 2019, VICTIM2 was interviewed by Special Agents assigned to HSI Office of Professional Responsibility in Seattle, WA. VICTIM2 advised that in late February 2019, she received a Facebook friend request from an individual by the name of "Tom Tuan Nguyen." VICTIM2 accepted the friend request and soon began regularly communicating with Nguyen, who purported himself to an Army doctor based in Kansas but

currently stationed in Syria. Throughout their relationship, Nguyen and VICTIM2 communicated by text message utilizing Facebook Messenger and Viber . VICTIM2 advised that Nguyen's Facebook page was under the name of Tom Dsung HU and his Viber number was (712)209-2067.

31. After approximately three weeks of communication, Nguyen told VICTIM2 that the government of Syria had given the soldiers on the mission a box containing seven million U.S. dollars and Nguyen asked VICTIM2 for her help in moving the box from Syria to Seattle, WA. VICTIM2 agreed and began planning with Nguyen how to move the box to the United States. Nguyen told VICTIM2 that shipping the box to Seattle, WA would cost $6,250 and the money would have to be sent to a man only known as "Jacob." On March 18, 2019, VICTIM2 deposited $6,250 into Bank of America account number 33405449573.

32. Nguyen also told VICTIM2 that the importation into the United States of this amount of currency required two U.S. Customs "Clearance Certificates" and these certificates cost 1% of the imported amount. Nguyen asked VICTIM2 to deposit $70,000 into Bank of America account number 334058917832 under the name Movaton Freight. VICTIM2 deposited this money on March 25, 2019.

33. Nguyen provided VICTIM2 with tracking number xcGFS4665490 for the box which he advised was shipped by Global Capital Finance & Courier Service. The company utilized email address info.GCFCS@usa.com to communicate with VICTIM2.

34. Additionally, Nguyen advised VICTIM2 about a Red Cross employee named Robert Breat who could assist in moving the box from Syria to the United States. Nguyen advised that Breat could help because the Red Cross moved cargo from Syria to the United States on a regular basis and Breat was familiar with the process. VICTIM2 stated that she text

messaged with Breat and his number was (620)273-3331. He also communicated with VICTIM2 using an email address of RC.Officer.R.Breat@deliveryman.com.

35. Nguyen also told VICTIM2 that he could not be released from his military duty without paying an early release penalty and he would also be required to finance his own travel back to the United States. According to Nguyen, his early release penalty was $47,250. VICTIM2 communicated with people purporting themselves to represent the U.S. Army utilizing an email address of U.S.ARMY-leavedept@usa.com. On March 28, 2019, VICTIM2 deposited $47,250 into Bank of America account number 388004018626 in the name of Logitech Group LLC. On April 3, 2019, VICTIM2 deposited an additional $7,200 into the same Logitech Group LLC bank account which she believed was to finance Nguyen's travel back to the United States.

36. In April 2019, Nguyen advised VICTIM2 that Breat had been arrested in New York as he tried to enter the United States from Syria. VICTIM2 received this information from Nguyen and subsequently received emails claiming such from email address U.S.Custom-Dept@usa.com. Nguyen said he knew a DHS employee named Marvin Najarro whom they could bribe to secure Breat's release. Nguyen told VICTIM2 the bribe would cost $170,000 and this would release Breat from custody and the box from being detained in New York. VICTIM2 said she was concerned about Breat's welfare and was not sure what else to do so she agreed to assist in bribing Najarro. Nguyen told VICTIM2 to deposit the money into Bank of America account number 898095871922. VICTIM2 told Nguyen she could not raise all the money but agreed to deposit $90,000 which she did on April 5, 2019. Nguyen advised VICTIM2 that his U.S. Army Commander's wife agreed to provide the other $80,000. VICTIM2 received text messages from Najarro who used phone numbers (913)336-1885 and (646)902-4036.

37. In early May 2019, Nguyen advised VICTIM2 that he would be coming to Seattle to secure the final release of the box and spend time with her. Nguyen sent VICTIM2 an itinerary that showed travel on Emirates Airlines from Beirut to Washington DC through Dubai at a cost of $1,444. The flight was departing Beirut on May 1, 2019 and arriving at Washington DC on May 2, 2019. On May 3, 2019, VICTIM2 traveled to the Seattle/Tacoma International Airport to pick up Nguyen. Nguyen and the box never arrived and VICTIM2 received no further communications. Shortly thereafter, the Facebook and phone numbers associated with Nguyen, Breat, and Najarro stopped working.

38. VICTIM2 advised that she did some research and discovered the picture that Nguyen had used for his Facebook profile was associated with an individual named Jayden Tran. VICTIM2 contacted Jayden Tran who advised that he had been previously contacted by people with similar narratives as VICTIM2 and that he didn't have any further information about the perpetrators.

39. On August 1, 2019, HSI received a response from 1&1 IONOS, Inc. which advised that the email addresses info.GCFCS@usa.com, RC.Officer.R.Breat@deliveryman.com, U.S.ARMY-leavedept@usa.com, and U.S.Custom-Dept@usa.com (collectively, Attachment A6) were all aliases under the same customer contract.

40. Therefore, VICTIM2 appears to have been victimized through a romance scam scheme which induced her to transfer sums of money to Logitech Group LLC under false or fraudulent pretenses.

INTERVIEW WITH VICTIM3

41. On August 6, 2019, Intelligence Research Specialist Laforte and I contacted VICTIM3 who was identified from having made three cash deposits on December 13, 2018

totaling $29,570 into Logitech Group LLC's Bank of America account. VICTIM3 recalled making the cash deposits into Logitech Group LLC's bank account and stated that she was scammed. VICTIM3 stated that she met a Vietnamese man named Johnson Nguyen on a dating website around November 2018. Nguyen claimed to be a U.S. Army solider serving in the Middle East. VICTIM3 communicated with Nguyen via Facebook Messenger. Nguyen requested that VICTIM3 send money to help children in a hospital in the Middle East. VICTIM3 was told by Nguyen that he would pay her back. VICTIM3 sent approximately $30,000 before realizing that she was being scammed. VICTIM3 advised that she deleted all of her communications with Nguyen and that she believes Nguyen's Facebook profile is no longer active. VICTIM3 was reluctant to continue talking about the incident and stated that it is very stressful for her to discuss.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

42. If issued, I anticipate executing the warrants for information under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). The company that each warrant is served to will be required to disclose to the government copies of the records and other information (including the content of communications) located at the premises described in Attachments A1 through A6 ("Property to Be Searched") and particularly described in Attachments B1 through B6, Part I ("Information to Be Disclosed"). Upon receipt of the information described in Part I of Attachments B1 through B6, government-authorized persons will review that information to locate the items described in Part II of Attachments B1 through B6 ("Information to be Seized by the Government").

CONCLUSION

43. Based on the foregoing, I respectfully submit that there is probable cause to believe that on the computer servers maintained by WhatsApp Inc., TextNow Inc., Oath Holdings Inc., Google LLC, AT&T, and 1&1 Mail & Media Inc within the accounts mentioned herein and set forth in Attachments A1 through A6, there exists evidence of violations of 18 U.S.C. § 1343 (wire fraud). I therefore respectfully request that the Court issue warrants authorizing the search of the accounts identified in Attachment A1 through A6 in order to seize and search the items listed in Attachment B1 through B6.

/s/ Derek Dunn
Special Agent Derek Dunn
Department of Homeland Security
Homeland Security Investigations

SUBSCRIBED TO AND SWORN BEFORE ME THIS 5th DAY OF NOVEMBER, 2019

/s/ Andrea K. Johnstone
Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A1

Property to be Searched

This warrant applies to information associated with WhatsApp account numbers **(978) 677-0918** and **(508) 581-7272** that is stored at premises controlled by WhatsApp Inc. of Menlo Park, California.

ATTACHMENT A2

Property to be Searched

This warrant applies to information associated with TextNow account number **(518) 730-9917** that is stored at premises controlled by TextNow Inc. of Waterloo, Ontario, Canada.

ATTACHMENT A3

Property to be Searched

This warrant applies to information associated with email address **shawnwalker909@yahoo.com** that is stored at premises controlled by Oath Holdings Inc. of Sunnyvale, California.

ATTACHMENT A4

Property to be Searched

This warrant applies to information associated with email address **kotara56@gmail.com** that is stored at premises controlled by Google LLC of Mountain View, California.

ATTACHMENT A5

Property to be Searched

This warrant applies to information associated with email address **shawnwalker909@yahoo.com** that is stored at premises controlled by Oath Holdings Inc. of Sunnyvale, California.

ATTACHMENT A6

Property to be Searched

This warrant applies to information associated with email addresses:

info.GCFCS@usa.com
RC.Officer.R.Breat@deliveryman.com
U.S.ARMY-leavedept@usa.com
U.S.Custom-Dept@usa.com

that is stored at premises controlled by 1&1 Mail & Media Inc of Chesterbrook, Pennsylvania.

ATTACHMENT B1
Particular Things to be Seized

I. Information to be disclosed by WhatsApp Inc. (the "Provider")

To the extent that the information described in Attachment A1 is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A1:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with each file, and the date and time at which each file was sent;

b. All transactional information of all activity of the account described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, methods of connecting, e-mails or "invites" sent or received, and any contact lists;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications with any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 for each account or identifier listed on Attachment A1, pertaining to the following matters, for the period December 1, 2013 through the present:

(a) Information that constitutes evidence of the identification or location of the user(s) of each account

(b) Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with each account about matters relating to the criminal activity under investigation, including records that reveal their whereabouts;

(c) Information that constitutes evidence indicating each account user's state of mind, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, related to the criminal activity under investigation;

(d) Information that constitutes evidence concerning how and when each account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account user;

(e) Information relating to bank transfers;

(f) Information relating to Logitech business, clients, sales, accounts, and employees;

(g) Information relating to the impersonation of other individuals.

ATTACHMENT B2
Particular Things to be Seized

II. Information to be disclosed by TextNow Inc. (the "Provider")

To the extent that the information described in Attachment A2 is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A2:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with each file, and the date and time at which each file was sent;

b. All transactional information of all activity of the account described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, methods of connecting, e-mails or "invites" sent or received, and any contact lists;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications with any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 for each account or identifier listed on Attachment A2, pertaining to the following matters, for the period December 1, 2013 through the present:

(a) Information that constitutes evidence of the identification or location of the user(s) of each account

(b) Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with each account about matters relating to the criminal activity under investigation, including records that reveal their whereabouts;

(c) Information that constitutes evidence indicating each account user's state of mind, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, related to the criminal activity under investigation;

(d) Information that constitutes evidence concerning how and when each account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account user;

(e) Information relating to bank transfers;

(f) Information relating to Logitech business, clients, sales, accounts, and employees;

(g) Information relating to the impersonation of other individuals.

ATTACHMENT B3
Particular Things to be Seized

III. Information to be disclosed by Oath Holdings Inc. (the "Provider")

To the extent that the information described in Attachment A3 is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A3:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with each file, and the date and time at which each file was sent;

b. All transactional information of all activity of the account described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, methods of connecting, e-mails or "invites" sent or received, and any contact lists;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications with any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 for each account or identifier listed on Attachment A3, pertaining to the following matters, for the period December 1, 2013 through the present:

(a) Information that constitutes evidence of the identification or location of the user(s) of each account

(b) Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with each account about matters relating to the criminal activity under investigation, including records that reveal their whereabouts;

(c) Information that constitutes evidence indicating each account user's state of mind, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, related to the criminal activity under investigation;

(d) Information that constitutes evidence concerning how and when each account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account user;

(e) Information relating to bank transfers;

(f) Information relating to Logitech business, clients, sales, accounts, and employees;

(g) Information relating to the impersonation of other individuals.

ATTACHMENT B4
Particular Things to be Seized

IV. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A4 is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A4:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with each file, and the date and time at which each file was sent;

b. All transactional information of all activity of the account described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, methods of connecting, e-mails or "invites" sent or received, and any contact lists;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications with any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 for each account or identifier listed on Attachment A4, pertaining to the following matters, for the period December 1, 2013 through the present:

a) All communications with an individual claiming to be Shawn Walker

b) All communications with the accounts: shawnwalker909@yahoo.com or (518)730-9917;

c) All communications related to Logitech

d) All communications related to bank transfers

ATTACHMENT B5
Particular Things to be Seized

V. Information to be disclosed by AT&T (the "Provider")

To the extent that the information described in Attachment A5 is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A5:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with each file, and the date and time at which each file was sent;

b. All transactional information of all activity of the account described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, methods of connecting, e-mails or "invites" sent or received, and any contact lists;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications with any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 for each account or identifier listed on Attachment A5, pertaining to the following matters, for the period December 1, 2013 through the present:

a) All communications with an individual claiming to be Shawn Walker

b) All communications with the accounts: shawnwalker909@yahoo.com or (518)730-9917;

c) All communications related to Logitech

d) All communications related to bank transfers

ATTACHMENT B6
Particular Things to be Seized

VI. Information to be disclosed by 1&1 Mail & Media Inc. (the "Provider")

To the extent that the information described in Attachment A6 is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A6:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with each file, and the date and time at which each file was sent;

b. All transactional information of all activity of the account described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, methods of connecting, e-mails or "invites" sent or received, and any contact lists;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications with any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1343 for each account or identifier listed on Attachment A6, pertaining to the following matters, for the period December 1, 2013 through the present:

(a) Information that constitutes evidence of the identification or location of the user(s) of each account

(b) Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with each account about matters relating to the criminal activity under investigation, including records that reveal their whereabouts;

(c) Information that constitutes evidence indicating each account user's state of mind, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, related to the criminal activity under investigation;

(d) Information that constitutes evidence concerning how and when each account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account user;

(e) Information relating to bank transfers;

(f) Information relating to Logitech business, clients, sales, accounts, and employees;

(g) Information relating to the impersonation of other individuals.